Cisco Secure Desktop ActiveX制御コード実行の脆弱性

severity

アドバイザリーID : cisco-sa-20100414-csd

初公開日 : 2010-04-14 16:00

バージョン 1.1 : Final

回避策 : No Workarounds available

Cisco バグ ID :

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco Secure Desktopには脆弱なActiveXコントロールが含まれており、攻撃者は該当システムに現在ログインしているユーザの権限で任意のコードを実行できる可能性があります。シスコはこの脆弱性に対処する無償のソフトウェアアップデートをリリースしました。この脆弱性を軽減する回避策があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100414-csd で公開されています。

該当製品

脆弱性のある製品

3.5.841よりも前のバージョンのCisco Secure Desktopが影響を受けます。

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

詳細

Cisco Secure Desktopで使用されるシスコ署名付きActiveXコントロールが、Cisco Secure Desktopのインストールプロセスで使用される実行可能ファイルの整合性を適切に検証できない

。攻撃者が攻撃者によって制御されたWebページにアクセスするようにユーザを誘導できる場合、脆弱なActiveXコントロールが起動され、攻撃者によって修正されたパッケージがダウンロードされる可能性があります。パッケージには、影響を受けるユーザの権限で実行される悪意のある実行可能ファイルが含まれている可能性があります。不正利用に成功すると、脆弱なシステムが完全に侵害される可能性があります。この脆弱性は、Cisco Bug ID CSCta25876 (登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2010-0589が割り当てられています。

回避策

管理者は、Microsoft Windowsのキルビット機能を使用して、脆弱性のあるActiveXコントロールのロードと実行を防止することで、この脆弱性を軽減できます。管理者は、脆弱なActiveXコントロールのクラス識別子(CLSID)を使用してコントロールを無効にする必要があります。影響を受けるCLSIDは次のとおりです。

705EC6D4-B138-4079-A307-EF13E4889A82

Microsoft Windowsでキルビットを設定する手順については、次のリンクを参照してください。

http://support.microsoft.com/kb/240797

注：キルビット設定は永続的です。Cisco Secure Desktopの機能を回復するには、設定を削除する必要があります。管理者がVPNポータルデバイスでCisco Secure Desktopソフトウェアを修正済みバージョンに更新した後、Cisco Secure Desktopソフトウェアをアップグレードできるようにするには、Microsoft Windowsクライアントからキルビットを削除する必要があります。キルビットが削除されると、修正済みのCisco Secure Desktopバージョンがインストールされるまで、クライアントが脆弱になる可能性があります。

更新：Cisco Secure Desktopソフトウェアバージョン3.5.1077は、脆弱性のある古いActiveX CLSIDを新しく発行されたCLSIDに置き換えます。新しいインストールと旧バージョンのCisco Secure Desktopからのアップグレードでは、新しいCLSIDが使用されます。クライアントシステムにソフトウェアアップグレードがインストールされると、管理者は安全かつ永続的に、環境内の古いCLSIDに対するActiveXキルビット回避策を実装できます。

ネットワーク内のCiscoデバイスに導入できる追加の緩和テクニックについては、このアドバイザリに関連するCisco適用対応策速報を参照してください。

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20100414-csd

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照し

て、問題の解決状況と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco Secure Desktopバージョン3.5.841は、次のリンクからダウンロードできます。

https://sec.cloudapps.cisco.com/support/downloads/go/ImageList.x?relVer=3.5.841&mdfid=280277835&sftType=CSD+package-+ASA+Distribution&optPlat=&nodecount=2&edesignator=null&modelName=Cisco+Secure+Desktop&treeMdfId=268438162&treeName=Security&modifmdfid=null&imname=&hybrid=&imst=&lr=Y

注：Cisco Secure Desktop(CSD)バージョン3.0および3.1は、Cisco IOSソフトウェアの特定のバージョンとCisco適応型セキュリティアプライアンス(ASA)ソフトウェアバージョン7.xでの動作に対してのみサポートされています。Cisco Secure Desktopバージョン3.2 ~ 3.5は、Cisco ASAソフトウェアバージョン8.xでの動作に対してのみサポートされています。Cisco Secure Desktopバージョン3.2 ~ 3.5をサポートされているCisco ASAソフトウェアバージョンで実行している場合は、Cisco Secure Desktopバージョン3.5.841にアップグレードすることをお勧めします。

Cisco Secure Desktopバージョン3.0および3.1の有効なソフトウェアライセンスをお持ちのお客様は、脆弱性のないソフトウェアへの移行手順について、次のアドレスに電子メールを送信する必要があります。

csd-activex-inquiry@cisco.com

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

この脆弱性は、TippingPointのZero Day Initiativeを担当する匿名の研究者によって発見され、シスコに報告されました。シスコは、この脆弱性を報告し、組織的な開示に協力していただいたTippingPoint社に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100414-csd

改訂履歴

リビジョン 1.1	2010年7月13日	回避策を更新。
リビジョン 1.0	2010年4月14日	初回公開リリース

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。